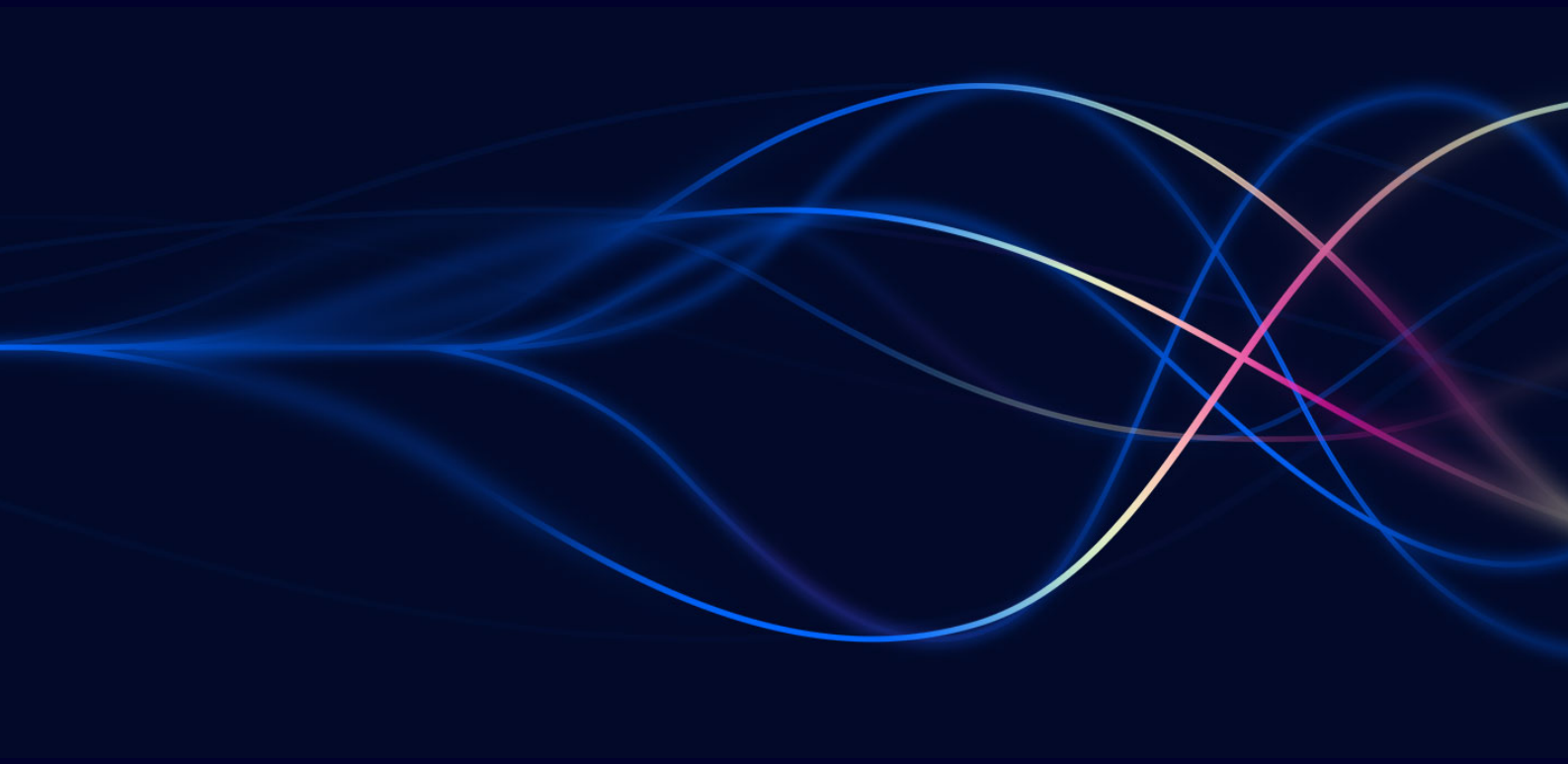
Q-FEEDS

Setup Guide
SonicWall NGFW

Public



Version 1.0 – 12 November 2024

Introduction

In today's world, keeping your network secure is super important. Next Generation Firewalls (NGFWs) are essential tools for protecting your network. They can filter DNS and web traffic using external dynamic lists of threat indicators, known as Indicators of Compromise (IoCs).

Q-Feeds provides dynamic, up-to-date lists of these IoCs, designed specifically for use with security controls like NGFWs. By integrating Q-Feeds into your SonicWall firewall, you can improve your network's protection against new and emerging threats. This means your firewall can automatically block harmful traffic and stay updated with the latest threat information.

This manual will show you how to set up and use Q-Feeds with your SonicWall firewall, so you can get the best security possible. You'll learn how to configure the firewall, import Q-Feeds, and ensure everything is working correctly. With these steps, you'll be able to enhance your network's defenses and keep your data safe from cyber threats.

Using Q-Feeds for Enhanced Network Security

Q-Feeds provides dynamic lists of Indicators of Compromise (IoCs) to enhance your network security controls. These lists, based on Q-Feeds Threat Intelligence Data Feeds, are regularly updated with various types of IoCs such as IP addresses and domains. By using these lists, you can monitor and block user access to dangerous network resources effectively.

Available Lists of Indicators

Q-Feeds offers the following types of indicators for SonicWall:

Name	Type	Description	URI
Malware IPs	IP	List of dangerous IP addresses	https://api.qfeeds.com/api?feed_type=malware_ips&api_token=XXXXXX&limit= XXXXXX

To optimize system performance and prevent unnecessary strain on our infrastructure, please schedule updates at the standard interval of 20 minutes. Setting the interval to less than 20 minutes is not beneficial and may overload the system.

Accessing the lists—including direct downloads into your network security solutions—requires an API token from Q-Feeds. You can request this token through your account manager or by visiting our website at https://qfeeds.com/start-trial-license/.

With the trial token, you will receive 30 days of free and full access to all our indicators of compromise. If you need assistance, please contact your account manager or email us at sales@qfeeds.com.

To test downloading the lists, you can use the cURL utility. Here is the syntax for Linux systems:

```
curl -v -u api_token:XXXXX
https://api.qfeeds.com/api?feed_type=malware_ips&limit=XXXXX
```

Setup Q-Feeds

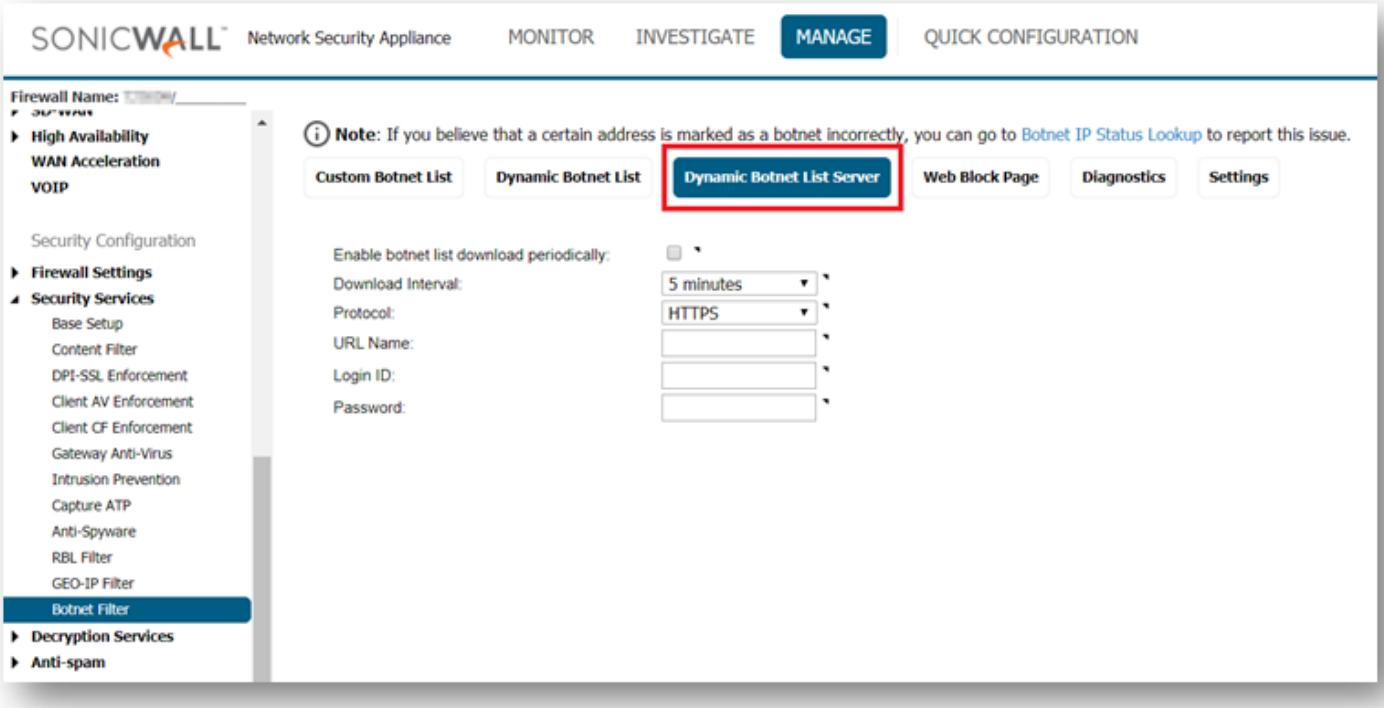
SonicWall Next-Generation Firewall operates on the SonicOS platform. The system supports the integration of external dynamic lists containing Indicators of Compromise (IoCs). These IoCs are managed as updatable text files hosted on a web server and accessible via HTTP or HTTPS.

With SonicOS 6.5.2, username and passwords for HTTP URLs in the dynamic Botnet configuration are accepted, and the information is transmitted in the HTTP header so the firewall has the required information.

After importing IoCs into your SonicWalls device, you can apply them as a Dynamic Botnet Filter in Firewall rules and such.

To configure this feature follow these steps:

1. Navigate to MANAGE → Security Configuration → Security Services → Botnet Filter.
2. Click on Dynamic Botnet List Server

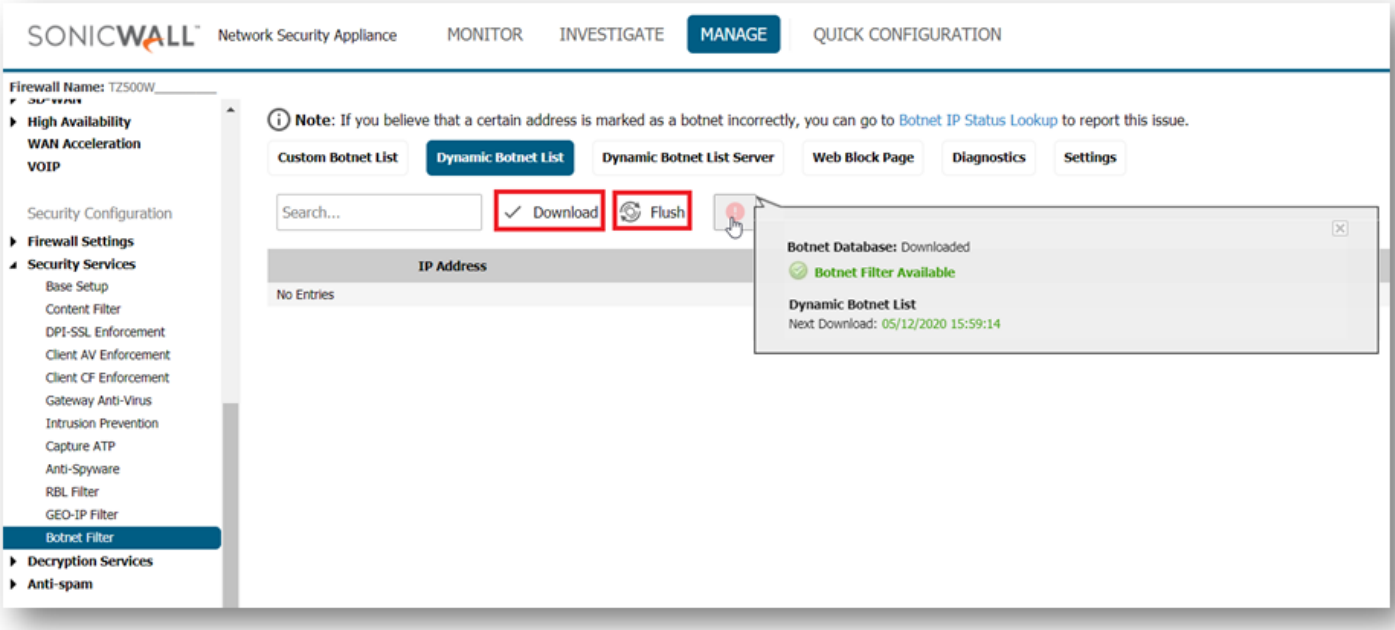


3. Select "**Enable** Botnet list Download periodically"
4. Select **15 minutes** for the update interval. Note: Q-Feeds only updates the feeds every 20 minutes so there might be updates without an update.
5. Select the protocol in which the firewall has to communicate with the backend server to retrieve the file from Protocol to **HTTPS**
6. URL name: **api.qfeeds.com/api?feed_type=XXXX&limit=XXXXX**
   replace "xxxx" with your feed type. Set **limit to 2000** (Important) due to memory limits

7. Enter the login ID **“api_token”**
8. Enter the **API token** which you have received from Q-Feeds as the password.

To view the downloaded list

1. Navigate to MANAGE → Security Configuration → Security Services → Botnet Filter
2. Navigate to the Dynamic Botnet List Tab
3. You can manually download the list immediately by clicking on the Download button or after the download interval, the IP addresses from the list will start showing up on this page.
4. You also have an option to Flush the entries downloaded via Dynamic Botnet List Server.
5. Any errors or misconfiguration can be seen on the button next to the Flush that explains what features are necessary to be ON for this to function as well when the next download is scheduled.



NOTE: When Dynamic Botnet List Server is configured, the SonicWall first inspects this list and when none of the IP matches, it checks the Botnet database from the back end to take further actions.

How to Configure Botnet Filtering with Firewall Access Rules

This part covers how to use SonicWall Botnet security service with access rule. This article will demonstrate how to create a firewall access rule for a mail server so that the mail server will be protected from going to a malicious IPS while the rest of the network traffic will be passed without being scanned by Q-Feeds. Pleae note that you can also apply these checks on web traffic.

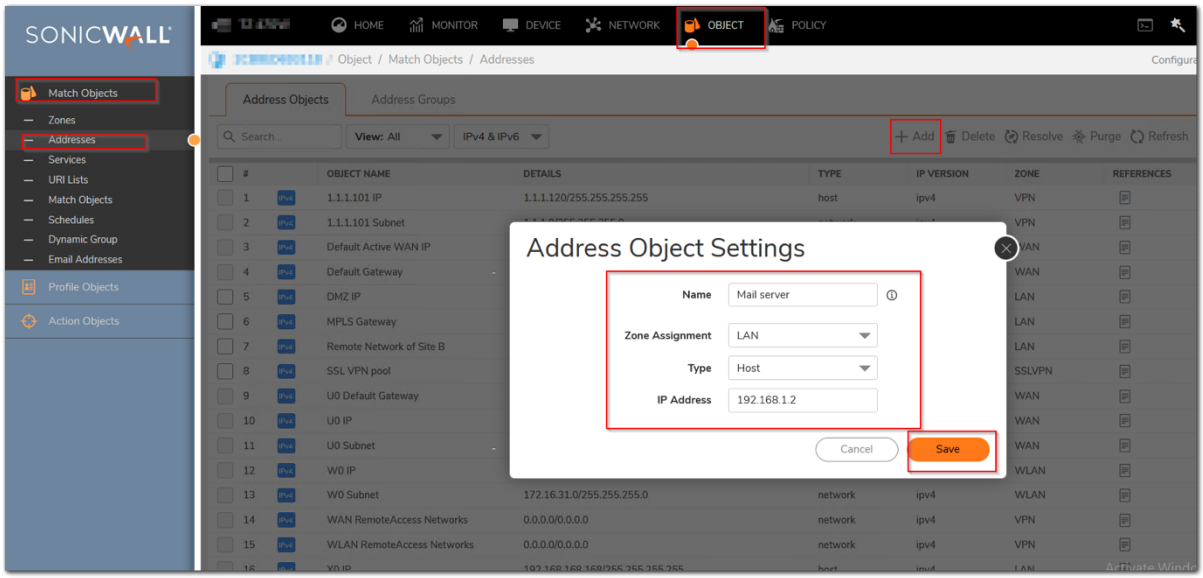
Resolution for SonicOS 7.X

Please scroll down for SonicOS 6.5

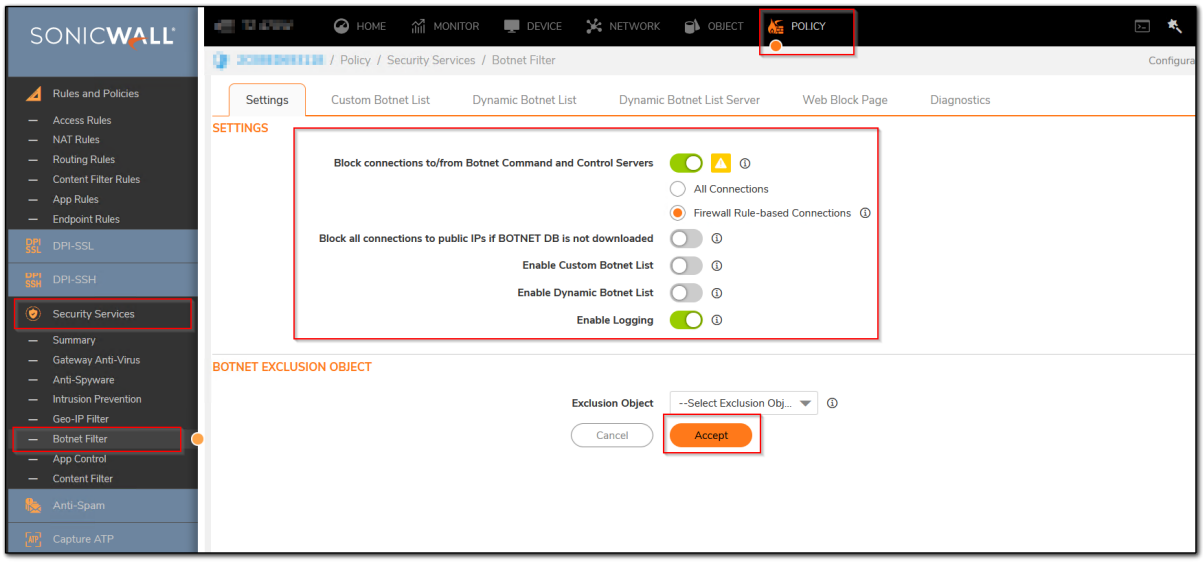
This release includes significant user interface changes and many new features that are different from the SonicOS 6.5 and earlier firmware. The below resolution is for customers using SonicOS 7.X firmware.

Steps to take:

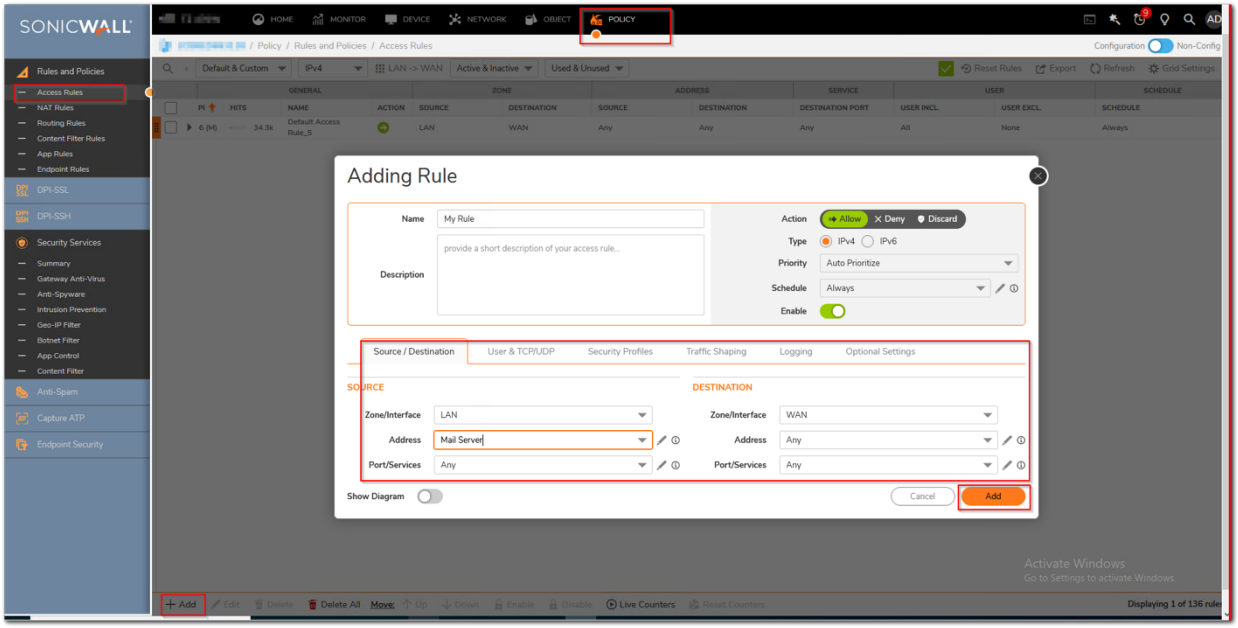
1. Create an Address Object for the Mail Server.
    a. Click OBJECT in the top navigation menu
    b. Navigate to Match Objects | Addresses
    c. Click on Add
    d. Enter the Mail Server IP address
    e. Click on Save

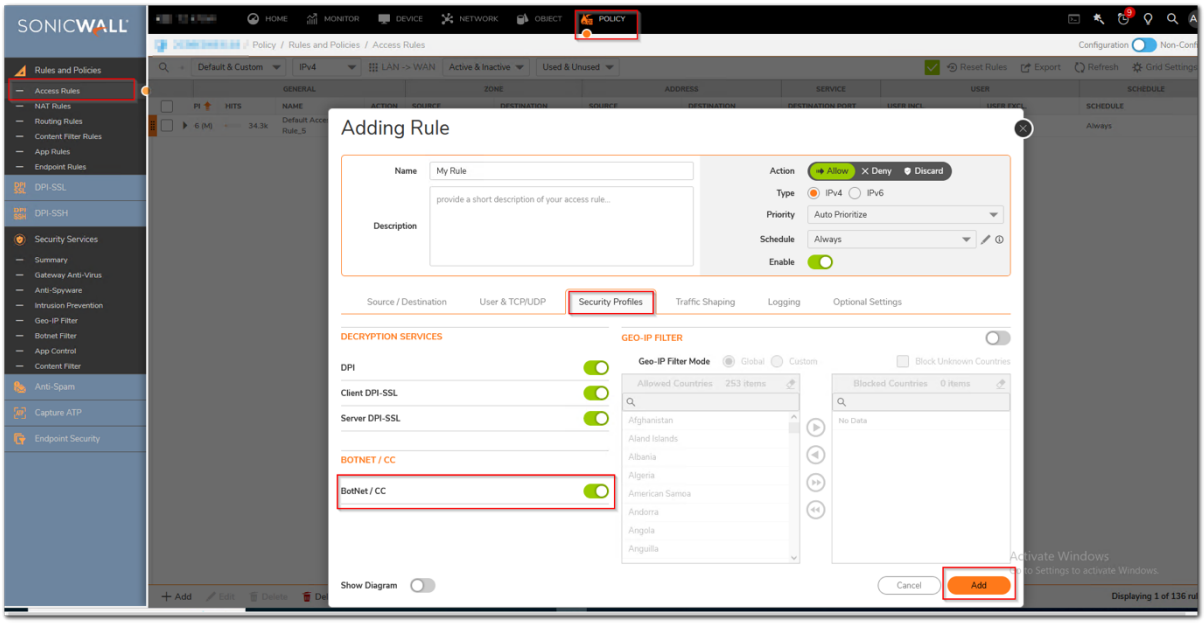


2. Click POLICY in the top navigation menu
    a. Navigate to Security Services | Botnet filter
    b. Enable Block connections to/from Botnet Command and Control Servers based on Firewall Rule-based Connections and Enable Logging
    c. Click on ACCEPT to Save



3. Create an Access Rule that we want to apply the Botnet Filter service to.
    a. Click POLICY in the top navigation menu
    b. Navigate to Rules and Policies | Access Rules
    c. Click on Add
    d. In our example we will create an access rule from the LAN>WAN to enable Botnet Filtering from the Mail Server.
    e. On Access rule navigate to Security Profiles, Enable BOTNET / CC
    f. Click on Add

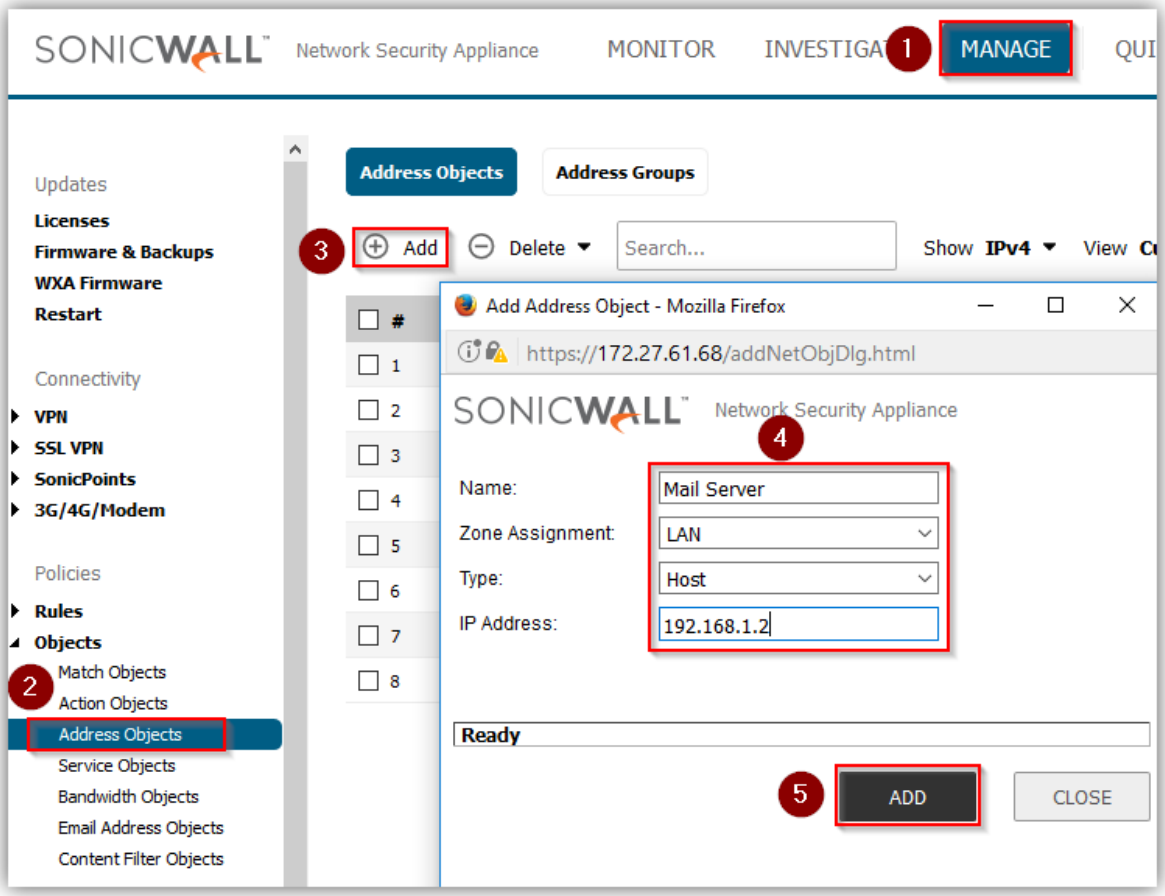




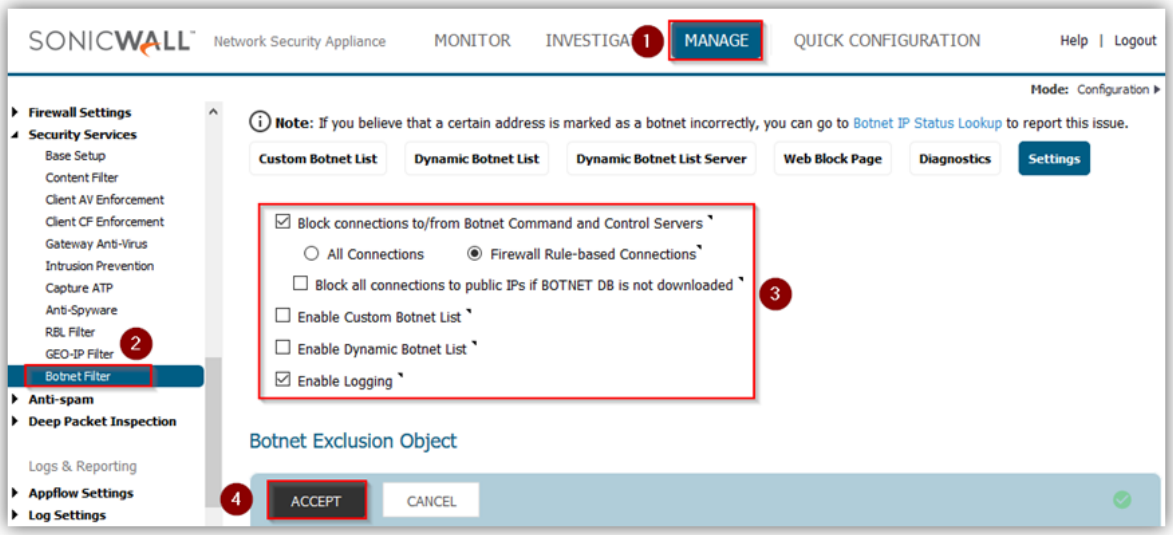
Resolution for SonicOS 6.5

Steps to take:

1. Create an Address Object for the Mail Server.
    a. Click Manage in the top navigation menu
    b. Navigate to Objects | Address Objects
    c. Click on Add
    d. Enter the Mail Server IP address
    e. Click OK to Save



2. Click MANAGE in the top navigation menu
    a. Navigate to Security Services | Botnet filter
    b. Enable Block connections to/from Botnet Command and Control Servers based on Firewall Rule-based Connections and Enable Logging
    c. Click on ACCEPT to Save



3. Create an Access Rule that we want to apply the Botnet Filter service to.
    a. Click MANAGE in the top navigation menu
    b. Navigate to Rules | Access Rules
    c. Click on Add
    d. In our example we will create an access rule from the LAN>WAN to enable Botnet Filtering from the Mail Server.
    e. On Access rule navigate to Security Profiles, Enable BOTNET / CC
    f. Click on Add